Séminaire de théorie des nombres

Le 31 mars 2014 à 14h (Jussieu)

Logarithmes discrets dans les corps finis de petite caractéristique

Exposé de Antoine Joux
(LIP6)

Résumé : Dans cet exposé, nous présenterons quelques avancées récentes qui ont permis d'améliorer très notablement le calcul de logarithmes discrets en petite caractéristique, à la fois en théorie et en pratique. Sur l'aspect théorique, on obtient sous réserve d'hypothèses heuristiques semblant raisonnables un algorithme de complexité quasi polynomiale dans la taille du corps considéré (si la caractéristique est suffisamment petite). Sur le plan pratique, ces nouvelles méthodes ont permis d'obtenir de nouveaux records en calculant des logarithmes discrets dans des corps auparavant considérés comme totalement inaccessibles.